69th ADA OIP Inspection Checklist – COMSEC

DATE	
UNIT INSPECTED	
INSPECTOR	
UNIT REPRESENTATIVE	

STANDARDS:
Commendable (C): 90-100% success rate of evaluated tasks
Satisfactory (S): 70-89%% success rate of evaluated tasks
Needs Improvement (N): 69% or less success rate of evaluated tasks

REFERENCES:
AR 380-40
AR 380-5
AR 600-25
AR 623-205
AR 25-50
AR 25-12
AR 380-67
AR 710-2
IAA 002-2010
NAG 71
NAG 53B9
NSA CSS EPL
TB 380-41
TB 750-38
DA PAM 25-16
DA PAM 25-380-2
DA PAM 25-35
AKMS Message #5

OVERALL RESULTS	**%**
COMMENDABLE	
SATISFACTORY	
NEEDS IMPROVEMENT	

69th ADA OIP Inspection Checklist – COMSEC

Performance Measures	Go	No-Go	N/A
The basis for approval of the facility, as reflected in the latest memorandum, "COMSEC Facility Approval Request," remains unchanged (AR 380-40, paraqraph 4-4).			
Review Command COMSEC inspections to ensure all discrepancies indicated on previous inspection reports have been reconciled lAW AR 380-40, paragraph 6-2.			
Have authorized systems users been assigned operator's privilege management responsibility accordingly with the account's highest security level (NAG 71, paragraph 21)?			
Maintenance personnel have been certified on DD Form 1435 per AR 25-12, chapters 3 & 4.			
The requirements for access to COMSEC information are known and adhered to (lAW AR 380-40, paragraphs 2-3) and clearances are verified per AR 380-67, chapter 7. a. Is there an access roster posted? b. For accounts that are only a safe, the access roster is the SF 700. c. Is security clearance of personnel on the access roster (SF 700) equal or higher to the classification of material held?			
The following documents are readily available or on requisition: AR 380-40, TB 380-41, AR 380-5, and AR 710-2/Unit Supply Update.			
Personnel understand the use of the marking "CRYPTO" (paragraph 5.1.5 and AR 380-40, paragraph 2-8). CRYPTO designator identifies all COMSEC key used to protect or authenticate information.			
COMSEC records are maintained lAW paragraph 4.3 and AR 380-40, Appendix C.			
All mandatory modifications to classified COMSEC equipment are applied and the equipment modification records plates accurately reflect their application lAW TB 750-38(C).			
Keying material is inventoried in a manner that assures continuous protection and control (paragraph 4.12c). a-. Daily inventory can be reverified with SF 702. b. Is daily inventory taken by Hand Receipt Holders? c. Is daily inventory for TS material initialed by two people?			
COMSEC material (including amendment residue) is destroyed in accordance with the schedule and procedures in chapter 6. Superseded key is completely destroyed by burning or by destruction devices and methods that meet the criteria in paragraph 4.19. a. Are Local Destruction Reports signed by two properly cleared people? b. Do consolidated destruction reports have back-up Local Destruction Reports?			
COMSEC publications, as required, are posted with the latest changes and amendments and are page checked (paragraph 4.4.6, 4.15.3 and DA PAM 25-35). a. Are the amendments posted within two days of receipt? b. Is the Record of Amendments page completed, to include amendment identification (i.e., for hard copy: amendment number, message amendments will be DTG, and letter amendments: LTR and date)? c. Were amendments posted in sequence?			
Local accounting procedures for issuing COMSEC material are known and properly implemented (paragraph 4.16). a. Are hand receipts (SF 153) properly completed? b. Is electronic key being issued on a local key control document (Le., DA Form 5941-E or DA Form 5251-E)?			
All cryptosystems and authentication systems used by the command are NSA approved (paragraph 3.3.4			

69th ADA OIP Inspection Checklist – COMSEC

All keying material on hand is being used on a routine basis or is held for valid contingency purposes (paragraph 3.4.2). a. Is key being destroyed without being used? b. Can operational key be changed to a contingency key?			
Amount of key held in the COMSEC account and at user level is restricted to the minimum required (paragraph 3.9 thru 3.9.5).			
If a secure room is used for operations, it meets the minimum requirements of paragraph 5.3.2 and AR 380-40, Appendix D. a. Does the account's CFAR accurately identify what is physically in place in the facility?			
When the COMSEC Facility is unoccupied, it is provided with safeguards that are deemed by the commander to afford proper protection against unauthorized access? (paragraph 5.7). a. Are locking bars being used on equipment loaded with classified key at unattended sights? b. Are locking bars used on classified equipment in mobile/transportable facilities? c. Are security containers securely affixed to mobile/transportable facilities?			
Unsecured telephones and other transmitting devices on site are actually required for operation (paragraph 5.3.4).			
Only mission essential, government owned tape recorders, radios, television receivers and cameras, etc. are authorized in the operational COMSEC Facility (paragraph 5.3.5b). a. Are there any personally owned electronic or duplicating devices in a operational COMSEC Facility? b. Has the local commander authorized, in writing, the use of radios, TVs ,etc?			
Installation and operation of electronic access control devices conform to the requirements of paragraph 5.3.5c. a. Does the facility door have another approved locking device in addition to the electronic? b. Has the combination been changed at least annually (recorded on an SF 700 attached to or near the door)?			
COMSEC key is stored as required by paragraph 5.8.1? a. Is TS material stored under TPI rules? b. Is open storage used for classified COMSEC key? If so, is open storage authorized lAW AR 380-40, 2-21.b?			
Location where classified CRYPTO key is stored is augmented by facilities that prevent unauthorized access to the storage container or vault itself lAW paragraph 5.8.3c? a. Do COMSEC Facilities consisting of no more than a safe(s) have a second barrier, such as a key lock in the door and controlled access to the keys? b. Has the TS area been declared a No-Lone-Zone? c. Are there controls on visual access (Le., drapes on windows, material in safes, inside cannot be seen from a common use area, etc.)?			
Containers used for storing classified COMSEC information meet original procurement specifications for physical security (paragraph 5.8.3b). a. Is TS material being stored in a previously damaged safe that has been restored to meet original specifications? b. For SECRET and below material, has a previously damaged safe been restored to meet original specifications?			

69th ADA OIP Inspection Checklist – COMSEC

Locks used to secure storage containers or to secure rooms are approved built-in combination locks or, where prescribed, are approved combination padlocks commensurate with the classification of material and circumstances (paragraph 5.8, 5.11.2(d) and AR 380- 40, paragraph D-3.d). a. Have all safes and Group 1-type locks been modified with the new electronic combination locks (XO?) lAW DA message DTG 232059Z NOV 93, SUBJECT: Retrofit Program for Security Locks? b. For unattended sites, is equipment secured with locking bars and secured by an electromechanical lock meeting Federal Specification FF-C-2740?			
When not installed in an operational configuration, classified crypto-equipment and components are stored securely (paragraph 5.8.4a). a. Is COMSEC crypto-equipment being stored with items of monetary value (Ie.,money, jewelry, etc.)? b. Are common fill devices being stored keyed when not specifically authorized?			
When installed in an operational configuration, unattended, un-keyed crypto equipment is left installed and protected in a manner approved by the commander lAW paragraph 5.8.4b? a. Is the vehicle or shelter containing the classified COMSEC equipment secured with a 5200 Series High Security Padlock or a combination lock? b. Is classified COMSEC equipment secured in its shelter mounting by a steel locking bar that is locked in place with combination padlocks meeting Federal Specification FF-P-110, Sergeant & Greenleaf Model 8077A (NSN 5340-00-285-6523)?			
All classified COMSEC documents are stored securely (paragraph 5.8.4e). a. Are all classified documents and equipment stored in a safe? b. Has the commander authorized, in writing, open storage of material classified SECRET and below (other than classified CRYPTO key)?			
Lock combinations have been changed within the past 12 months or when an individual knowing the combination no longer requires access (AR 380-5, paragraph 5-104.b and AR 380-40, paragraph 4-5.g). a. Is the SF 700 properly classified? b. Is the SF 700 signed and dated? c. Are there two SF 700s for TS safes?			
Lock combinations are disseminated to an absolute minimum number of authorized personnel (paragraph 5.8.4h(3)).			
Access to the COMSEC Facility is granted and controlled lAW the provisions of paragraph 5.2a and AR 380-40, paragraph 4-5.d. a. Is there a COMSEC Facility access roster posted or on file in the account? b. Do the people having access have the appropriate security clearances? c. Are visitors required to sign the Restricted Area Visitors Register (DA Form 1999-E)? d. Is the DA Form 1999-E signed by the authorizing official and IN/OUT times recorded?			

69th ADA OIP Inspection Checklist – COMSEC

Daily security checks are made at the end of each workday and on non-workdays, as required (paragraph 5.4.1 and 5.4.2). a. If the COMSEC Facility is a room/building, is an SF 701 being maintained? b. Is the SF 702 being maintained correctly (Le., "checked by" block always filled out, whether opened or not; not required if the room is not entered)? (The "checked by" block can be initialed by the same person that locked the safe, if no one else is available.) c. For TS safes, are there two SF 702s: one for each combination?			
The procedures for preparing classified COMSEC material for shipment are known and adhered to (paragraph 5.10.1).			
Authorized means of transporting classified COMSEC material are known and adhered to (paragraph 5.10.2 and AR 380-40, paragraph 2-17).			
Where applicable, an emergency plan has been prepared and includes those provisions of paragraph 5.16.1 deemed appropriate by the commander (AR 380-40, paragraph 3-4). a. For OCONUS accounts, is there an emergency plan prepared? b. Is the plan workable (i.e., how/where are safe combinations located, how do you carry large quantities of COMSEC material, where do you get a vehicle, how do you start a fire, etc.)?			
The emergency plan is compatible with command emergency plans (paragraph 5.16.2), and emergency procedures provide for the immediate destruction of superseded key lAW paragraph 5.18.5. a. Has the emergency plan been coordinated with those units involved?			
The emergency plan is compatible with command emergency plans (paragraph 5.16.2), and emergency procedures provide for the immediate destruction of superseded key lAW paragraph 5.18.5. a. Has the emergency plan been coordinated with those units involved?			
Emergency destruction materials are adequate and readily available for use (paragraph 5.18.5). a. Are the destruction devices located where the emergency plan indicates they are?			
Where applicable, briefings and dry runs are held quarterly (and documented), and all personnel are aware of their responsibilities in the event of an emergency (AR 380-40, paragraph 3-5 and TB 380-41, paragraph 5.15b). a. Are there at least four dry run documents on file?			
Sensitive pages of COMSEC maintenance manuals (KAMs) have been prepared for quick removal, where required, and personnel are familiar with the emergency implementing procedures (paragraph 5.19). a. Have the upper corners of sensitive pages been cut off?			
Personnel are familiar with reportable incidents pertaining to the cryptosystems and associated material held (paragraph 7.1 and AR 380-40, paragraph 7-3). a. Is destruction documentation properly filled out, to include two signatures? b. Has keying material been destroyed within 72 hours of supersession? c. Is classified material properly secured? d. Do users have proper security clearances for material being used?			
Supervisory personnel are thoroughly familiar with the requirements for reporting incidents (paragraph 7.1 and AR 380-40, paragraph 7-6).			

69th ADA OIP Inspection Checklist – COMSEC

Users are aware of the requirement to report directly to the appropriate CONAUTH all circumstances, occurrences, or acts that could lead to a compromise of key (paragraph 7.1 and AR 380-40, paragraph 7-1). a. Do COMSEC personnel know who the CONAUTH is for the material held? b. Is the COMSEC Custodian the CONAUTH for any of the material held?			
All centrally accountable COMSEC material on hand, including the number of copies or items, is mission essential (AR 380-40, paragraph 5-3). a. Is the COMSEC Custodian conducting an annual review of key being held? b. Is there any key being destroyed on a monthly base that is not being used?			
Annual review by CONAUTH is accomplished and the required documentation is on hand (T8 380-41, paragraph 3.6.7a). a. Is the report for the annual review of key on file in the account?			
REMARKS:			